Kapitola 3

Řešení lineárních kongruencí, primitivní kořeny, Eulerova funkce

3.1 Opakování z přednášky

Řešíme kongruenci $a' x \equiv b' \pmod{n'}$. Můžeme si ji vydělit $d := (a', b', n')$ a dostat kongruenci

$$a x \equiv b \pmod{n}$$

kterou si převedeme přidáním vždy platné kongruence na soustavu

$$\begin{aligned} a x &\equiv b \pmod{n} \\ n x &\equiv 0 \pmod{n} \end{aligned}$$

a tu ekvivalentními úpravami převedeme do tvaru

$$\begin{aligned} x &\equiv c \pmod{n} \\ 0 x &\equiv e \pmod{n} \end{aligned}$$

kde následně máme dvě možnosti:

- $e \equiv 0 \pmod{n}$, pak $x \equiv c \pmod{n}$ je řešení, modulo n' pak máme d řešení: $x \equiv c$, $x \equiv c + n$, $c + 2n$, $\ldots$, $x \equiv c + (d-1)n \pmod{n'}$;
- $e \not\equiv 0 \pmod{n}$, pak původní kongruence nemá řešení.

Soustavu kongruencí (mají-li každá jednotlivě řešení) si můžeme podle předchozího vždy převést do tvaru

$$\begin{aligned} x &\equiv c_1 \pmod{n_1} \\ x &\equiv c_2 \pmod{n_2} \end{aligned}$$

$$\vdots$$
$$x \equiv c_k \pmod{n_k}$$

která má řešení právě tehdy, když $c_i \equiv c_j \pmod{(n_i, n_j)}$. Toto řešení je pak jediné modulo $[m_1, \ldots, m_k]$. Soustavu řešíme tak, že si (třeba) z první kongruence vyjádříme parametricky $x = n_1 t_1 + c_1$, což následně dosadíme do (třeba) druhé kongruence, kterou vyřešíme vzhledem k t_1, tedy $t_1 = m_2 t_2 + c_2'$, což následně dosadíme za x a dosadíme do (například) třetí kongruence a postup iterujeme.

Eulerova funkce φ je pro přirozené číslo n zadaná následujícím předpisem

$$\varphi(n) = \left|\{m \in \mathbb{N} \mid m \leq n \text{ a } (m, n) = 1\}\right|.$$

Je celkem zřejmé, že pro prvočíslo p je $\varphi(p) = p - 1$. Dále $\varphi(p^k) = p^{k-1} \cdot (p-1)$. Eulerova funkce je *multiplikativní*, tj. pro a, b taková, že $(a, b) = 1)$ máme $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$. Napíšeme-li si tedy n jako součin mocnin prvočísel

$$n = p_1^{k_1} \cdot \cdots \cdot p_l^{k_l}$$

můžeme spočítat

$$\varphi(n) = p_1^{k_1 - 1} \cdot (p_1 - 1) \cdot \cdots \cdot p_l^{k_l - 1} \cdot (p_l - 1).$$

Věta (Eulerova)**.** *Pro a, n taková, že $(a, n) = 1$ platí $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Věta (malá Fermatova)**.** *Pro prvočíslo p a a jím nedělitelné platí $a^{p-1} \equiv 1 \pmod{p}$.*

Pro a a n taková, že $(a, n) = 1$ číslo r nazveme *řádem a modulo n*, jestliže se jedná o nejmenší číslo takové, že $a^r \equiv 1 \pmod{n}$, neboli pokud $a^{r'} \equiv 1 \pmod{n}$, pak $r \mid r'$. Existence řádu je zaručená Eulerovou větou.

Věta (Lagrangeova[1])**.** *Řád čísla a modulo n dělí $\varphi(n)$.*

Číslo a je *primitivní kořen modulo n*, jestliže pro každé b existuje k takové, že $a^k \equiv b \pmod{n}$.

Věta. *Primitivní kořen modulo prvočíslo existuje.*

Při hledání primitivního modulo p je potřeba najít číslo, jehož řád je právě $\varphi(p) = p - 1$. Díky Lagrangeově větě si můžeme vypsat všechny dělitele $p - 1$ do Hasseovského diagramu (uspořádaného dělitelností), kde následně stačí testovat modulo p „submaximální“ mocniny čísel a, tj. takové, které v Hasseovském diagramu leží těsně pod $p - 1$. Pokud by totiž byla kongrentní jedné i menší mocnina a, byla by jedné kongruentní i některá „submaximální“ mocnina.

[1] Jedná se o speciální případ Lagrangeovy věty o konečných grupách. Ta říká, že řád prvku grupy dělí řád grupy.

3.2 Příklady řešené na cvičení

Příklad 3.1. Vyřešte kongruenci $74\,x \equiv 22 \pmod{168}$.

Řešení. Kongruenci si můžeme přepsat do tvaru $37\,x \equiv 11 \pmod{84}$. Protože $(37, 84) = 1$, má kongruence jediné řešení. Přidáme si platnou kongruenci $84\,x \equiv 0 \pmod{84}$ a ekvivalentními úpravami řešíme soustavu kongruencí.

$$\left.\begin{aligned} 37\,x &\equiv 10 \\ 84\,x &\equiv 0 \end{aligned}\right\} \pmod{84}$$
$$\left.\begin{aligned} 10\,x &\equiv -22 \\ 37\,x &\equiv 11 \end{aligned}\right\} \pmod{84}$$
$$\left.\begin{aligned} 10\,x &\equiv -22 \\ -3\,x &\equiv 15 \end{aligned}\right\} \pmod{84}$$
$$\left.\begin{aligned} x &\equiv 23 \\ -3\,x &\equiv 15 \end{aligned}\right\} \pmod{84}$$
$$\left.\begin{aligned} x &\equiv 23 \\ 0\,x &\equiv 84 \end{aligned}\right\} \pmod{84}$$

Vidíme, že $x \equiv 23 \pmod{84}$. Pak $x \equiv 23$ nebo $107 = 84 + 23 \pmod{168}$. Skutečně

$$74 \cdot 23 = 1\,702 = 1\,680 + 22 \equiv 22 \pmod{168}$$
$$74 \cdot 107 = 74 \cdot 84 + 74 \cdot 23 = 37 \cdot 168 + 74 \cdot 23 \equiv 22 \pmod{168}$$

tedy máme dvě řešení modulo 168. △

Příklad 3.2. Vyřešte soustavu kongruencí

$$\begin{aligned} x &\equiv 10 \pmod{25} \\ x &\equiv 6 \pmod{11}. \end{aligned}$$

Řešení. Jelikož $(25, 11) = 1$, má podle Čínské zbytkové věty soustava řešení, a to mezi 0 a $11 \cdot 25 = 275$ jediné. Jedním ze způsobů řešení je vypisovat si do tabulky čísla tvaru $25\,k + 10$ a čísla tvaru $11\,l + 6$. Máme hodnoty

$$x \in \{10, 35, 60, 85, 110, 135, 160, 185, 210, 235, 260\}$$

a

$$x \in \{6, 17, 28, 39, 50, 61, 72, 83, 94, 105, 127, 138, 149, 160, \dots\}$$

přičemž vidíme, že $x = 160$ a dále počítat nemusíme. Tento způsob je jednoduchý, nicméně procházet mnoho čísel bývá zdlouhavé.

Jinou možností je spočítat si Bézoutovy koeficienty pro čísla 25 a 11. Máme $1 = 4 \cdot 25 - 9 \cdot 11$ (ověřte sami), takže můžeme říci, že $4 \cdot 25 \equiv 1 \pmod{11}$ a $-9 \cdot 11 \equiv 1 \pmod{25}$. Můžeme v obou rovnicích představit jedničku, tedy

$$\begin{aligned} x &\equiv -9 \cdot 11 \cdot 10 \pmod{25} \\ x &\equiv 4 \cdot 25 \cdot 6 \pmod{11} \end{aligned}$$

přičemž každá z hodnot je kongruentní nule vůči druhému modulu. Vidíme tedy, že

$$x \equiv -9 \cdot 10 \cdot 11 + 4 \cdot 25 \cdot 6 = -390 \equiv 160$$

modulo 25 i modulo 11, tedy také modulo $11 \cdot 25 = 275$.

Třetí metodou řešení je vyjádřit si z první rovnice x parametricky a dosadit do rovnice druhé. Z první rovnice vidíme, že $x = 25\,k + 10$. Poté řešíme

$$\begin{aligned} 25\,k + 10 &\equiv 6 \pmod{11} \\ 3\,k - 1 &\equiv 6 \pmod{11} \end{aligned}$$

neboť $25 \equiv 3$ a $10 \equiv -1 \pmod{11}$, pak

$$\begin{aligned} 3\,k &\equiv 7 \pmod{11} \\ k &\equiv 6 \pmod{11} \end{aligned}$$

kde v posledním kroku jsme si vynásobili kongruenci 4, jelikož $3 \cdot 4 = 12 \equiv 1$ a $7 \cdot 4 = 28 \equiv 6 \pmod{11}$, a tedy $k = 11\,l + 6$. Celkem

$$x = 25\,k + 10 = 25\,(11\,l + 6) + 10 = 275\,l + 160,$$

čímž dostáváme řešení $x \equiv 160 \pmod{275}$. △

Příklad 3.3. Vyřešte soustavu kongruencí

$$\begin{aligned} x &\equiv 1 \pmod{15} \\ x &\equiv 4 \pmod{21} \\ x &\equiv 6 \pmod{25}. \end{aligned}$$

Řešení. Řešíme pouze metodou parametrického dosazování. Z první kongruence vyjádříme $x = 15\,k + 1$, dosazením do druhé kongruence získáme

$$\begin{aligned} 15\,k + 1 &\equiv 4 \pmod{21} \\ 15\,k &\equiv 3 \pmod{21} \end{aligned}$$

odtud zkrácením obou stran kongruence i modulu třemi

$$5\,k \equiv 1 \pmod{7}$$

$$k \equiv 3 \pmod 7$$

čímž dostáváme tři řešení, $k \equiv 3$, $k \equiv 10$ a $k \equiv 17 \pmod{21}$, nicméně všechna tato řešení lze psát dohromady jako $k = 7\,l + 3$. Máme tedy

$$x = 15\,k + 1 = 15\,(7\,l + 3) + 1 = 105\,l + 46$$

což dosadíme do třetí kongruence

$$\begin{aligned} 105\,l + 46 &\equiv 6 \pmod{25} \\ 105\,l &\equiv -40 \pmod{25} \\ 5\,l &\equiv 10 \pmod{25} \end{aligned}$$

neboť $105\,l \equiv 105\,l - 25 \cdot 4\,l = 5\,l$ a $-40 \equiv -40 + 2 \cdot 25 = 10 \pmod{25}$, dále zkrácením obou stran kongruence i modulu pěti

$$l \equiv 2 \pmod 5$$

takže máme řešení. Modulo 25 bychom dostali 5 řešení, $l \equiv 2$, 7, 12, 17 nebo $22 \pmod{25}$, nicméně všechna lze psát jako $l = 5\,t + 2$. Dosadíme tedy do x

$$x = 105\,l + 46 = 105\,(5\,t + 2) + 46 = 525\,t + 256$$

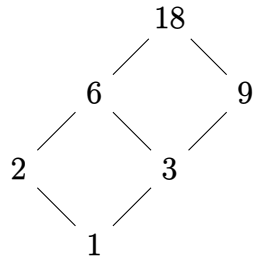
a máme řešení $x \equiv 256 \pmod{525}$, přičemž $525 = [15, 21, 25]$. Skutečně

$$\begin{aligned} 256 &= 1 + 15 \cdot 17 \\ &= 4 + 21 \cdot 12 \\ &= 6 + 25 \cdot 10 \end{aligned}$$

a jedná se o řešení. △

Příklad 3.4. Najděte primitivní kořen modulo 19 a modulo 53. Poté popište *všechny* primitivní kořeny.

Řešení. Protože 19 i 53 jsou prvočísla, v obou případech primitivní kořeny existují. Nejprve počítejme modulo 19. Podle Fermatovy věty pro každé $k \in \mathbb{N}$ máme $k^{18} \equiv 1 \pmod{19}$. Máme právě $18 = \varphi(19)$ čísel nesoudělných s 19, takže mají-li různé mocniny primitivního kořene dát všechny třídy kongruence, musí mít primitivní kořen řád 18. Řád obecného čísla modulo 19 je dělitelem 18 (Lagrangeova věta), tedy čísla mohou mít řád 1, 2, 3, 6, 9 nebo 18. Nakreslíme si Hasseovský diagram dělitelů 18 uspořádaný dělitelností



(3.1)

odkud vidíme, že stačí najít a takové, že a^6 ani a^9 není kongruentní 1 modulo 19. Pokud by totiž byla kongruentní jedné menší (v diagramu (3.1)) mocnina a, byla by 1 kongruentní i mocnina šestá nebo devátá. Hledáme tedy takové a. Jedna to nebude, zkusíme dvojku:

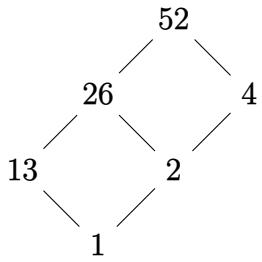
$$2^6 = 64 \equiv 7 \pmod{19}$$

neboť $19 \cdot 3 = 57$, dále

$$2^9 = 2^{6+3} = 2^6 \cdot 2^3 \equiv 7 \cdot 8 = 56 \equiv -1 \pmod{19}$$

kde jsme využili předchozího. Má tedy 2 řád 18 a je primitivním kořenem modulo 19. Ostatní primitivní kořeny jsou ty mocniny 2, kde je exponent nesoudělný s 18. Dále jsou primitivními kořeny tedy $2^5 \equiv 13$, $2^7 \equiv 14$, $2^{11} \equiv 15$, $2^{13} \equiv 3$ a $2^{17} \equiv 10 \pmod{19}$. Obecně počet primitivních kořenů bude $\varphi(18) = 6$.

Pro primitivní kořen modulo 53 hledáme číslo řádu 52, obecně mohou mít čísla řád 1, 2, 4, 13, 26 nebo 52. Nakreslíme si opět Hasseovský diagram dělitelů $52 = 13 \cdot 4$.



(3.2)

a vidíme, že stačí ověřovat čtvrtou a 26. mocninu. Můžeme zkoušet různá čísla, začneme opět dvojkou:

$$2^4 = 16$$

což není kongruentní 1, dále $2^6 = 64 \equiv 11 \pmod{53}$, tudíž

$$2^{26} = 2^{6 \cdot 4 + 2} = (2^6)^4 \cdot 2^2 \equiv 11^4 \cdot 4 = (11^2)^2 \cdot 4 \pmod{53}$$

s využitím $11^2 = 121 \equiv 15 \pmod{53}$ máme

$$2^{26} \equiv 15^2 \cdot 4 = 15 \cdot (15 \cdot 4) = 15 \cdot 60 \equiv 15 \cdot 7 = 105 \equiv -1 \pmod{53}$$

kde jsme využili, že $60 \equiv 7 \pmod{53}$ a $2 \cdot 53 = 106$. Tudíž 2 má řád 52 a je primitivním kořenem modulo 53. Ostatní primitivní kořeny jsou právě ty mocniny 2, kde exponent je nesoudělný s 52. Je jich $\varphi(52) = 24$. △

Příklad 3.5. Určete $\varphi(10)$, $\varphi(100)$, $\varphi(1\,000)$ a $\varphi(256)$.

Řešení. Počítáme podle vzorců

$$\varphi(10) = \varphi(2) \cdot \varphi(5) = 1 \cdot 4 = 4,$$

u 10 by to šlo i odhadnout, nesoudělná jsou 1, 3, 7 a 9,

$$\begin{aligned}\varphi(100) &= \varphi(2^2)\cdot\varphi(5^2) = 1\cdot 2\cdot 4\cdot 5 = 40,\\ \varphi(1\,000) &= \varphi(2^3)\cdot\varphi(5^3) = 1\cdot 4\cdot 4\cdot 25 = 400,\\ \varphi(256) &= \varphi(2^8) = 1\cdot 2^7 = 128,\end{aligned}$$

čímž máme hodnoty spočítány. △

Příklad 3.6. Nalezněte všechna $m\in\mathbb{N}$ taková, že $\varphi(m)=38$, respektive $\varphi(m)=16$.

Řešení. Máme rozklad $38=2\cdot 19$. Má-li $p\mid m$, musí $p-1\mid 38$. Protože $19+1=20$ není prvočíslo, musí být $p-1=2$, tedy $p=3$. Pak by mělo být $m=3^k$, nicméně pak

$$\varphi(m)=2\cdot 3^{k-1}=2\cdot 19$$

přičemž 19 není mocnina 3. Tudíž takové m neexistuje.

Pro $\varphi(m)=16$ máme $p\mid m\Rightarrow p-1\mid 16$, a pokud by p dělilo m i ve vyšší mocnině, muselo by pak i $p\mid 16$. Děliteli 16 jsou 1, 2, 4, 8 a 16, mezi nimiž hledáme $p-1$. Pak p může být 2, 3, 5 nebo 17 (9 není prvočíslo), přičemž jedině 2 se může vyskytovat i ve vyšší mocnině. Můžeme si tedy rozepsat $m=2^a\cdot 3^b\cdot 5^c\cdot 17^d$, kde b, c, $d\in\{0,1\}$. Procházíme všechny případy.

I) Nejprve vyřešme případ $17\mid m$. Poté $m=17\,k$ a $\varphi(m)=\varphi(17)\cdot\varphi(k)=16\,\varphi(k)=16$, tedy $\varphi(k)=1$, tudíž $k=1$ nebo 2. Máme tedy $m=17$ nebo 34.

II) Pokud 17 nedělí m, máme $m=2^a\cdot 3^b\cdot 5^c$, kde b, $c\in\{0,1\}$, tedy máme čtyři možnosti kombinací b a c, podle nichž vždy dopočítáme a. Pak máme

   i) $b=c=0$: $m=2^a$ a $\varphi(m)=1\cdot 2^{a-1}=16=2^4$, tedy $a=5$ a $m=32$;

   ii) $b=1$, $c=0$: $m=2^a\cdot 3$ a $\varphi(m)=2\cdot 2^{a-1}=16$, pak $a=4$ a $m=48$;

   iii) $b=0$, $c=1$: $m=2^a\cdot 5$ a $\varphi(m)=2^{a-1}\cdot 4=16$, $a=3$ a $m=40$;

   iv) $b=c=1$: $m=2^a\cdot 3\cdot 5$ a $\varphi(m)=2^{a-1}\cdot 8=16$, tudíž $a=2$ a $m=60$.

Dohromady pak může být $m\in\{17,32,34,40,48,60\}$. △